(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0083145
(43) 공개일자 2020년07월08일

(51) 국제특허분류(Int. Cl.)
H04L 29/08 (2006.01)
(52) CPC특허분류
H04L 67/1057 (2013.01)
H04L 67/1065 (2013.01)
(21) 출원번호 10-2019-0075373
(22) 출원일자 2019년06월25일
심사청구일자 2019년06월25일
(30) 우선권주장
1020180172455 2018년12월28일 대한민국(KR)

(71) 출원인
연세대학교 산학협력단
서울특별시 서대문구 연세로 50 (신촌동, 연세대학교)
(72) 발명자
정종문
서울특별시 용산구 이촌로 181, 104동 101호(이촌동, 한강대우아파트)
김형대
서울특별시 동작구 여의대방로16길 1, 104동 1003호(신대방동, 태성대아파트)
윤주식
서울특별시 서대문구 신촌로7길 49-6, 202호(창천동, 청송빌)
(74) 대리인
민영준

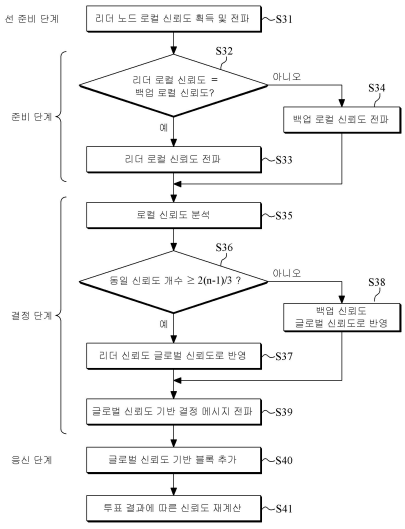
전체 청구항 수 : 총 5 항

(54) 발명의 명칭 **블록체인 네트워크의 합의 방해요인 제거를 위한 장애 허용 합의 방법**

(57) 요 약

본 발명은 블록체인 검증 노드의 투표 정보를 바탕으로 비정상 노드에 대한 패널티를 적용하여 합의 경계를 가변함으로써, 합의 교착상태에 들어가도 정상 노드와 비정상 노드의 투표권을 조정하여 정상 합의로 회귀할 수 있는 블록체인 네트워크의 장애 허용 합의 방법을 제공할 수 있다.

대 표 도 - 도3



이 발명을 지원한 국가연구개발사업

과제고유번호	1711076385
부처명	과학기술정보통신부
연구관리전문기관	정보통신기술진흥센터
연구사업명	대학 ICT 연구센터 지원사업
연구과제명	블록체인 비즈니스 서비스 기술 개발 및 인력양성
기 여 율	1/1
주관기관	중앙대학교 산학협력단
연구기간	2018.07.01 ~ 2021.12.31

명 세 서

청구범위

청구항 1

n개의 검증 노드 중 기지정된 리더 노드가 적어도 하나의 클라이언트로부터 전송된 트랜잭션 요청이 포함된 블록이 수신되면, 상기 리더 노드에 대해 이전 투표 결과로부터 획득된 로컬 신뢰도인 리더 신뢰도를 상기 블록에 포함하여 나머지 검증 노드인 백업 노드들로 전파하는 단계;

상기 백업 노드들 각각이 이전 투표 결과로부터 획득된 자신에 대한 로컬 신뢰도인 백업 신뢰도와 상기 리더 신뢰도를 비교하여, 서로 상이하면 다른 검증 노드들로 리더 신뢰도를 상기 백업 신뢰도로 변경한 준비 메시지를 전파하는 단계;

상기 검증 노드들 각각이 수신한 준비 메시지를 분석하여, 동일한 값을 갖는 로컬 신뢰도의 개수가 기지정된 기준 개수 이상이면, 다른 검증 노드들로 상기 로컬 신뢰도를 글로벌 신뢰도에 적용하여 결정 메시지를 전파하는 단계; 및

상기 검증 노드들 각각이 결정 메시지에 포함된 글로벌 신뢰도의 합을 기반으로 트랜잭션 요청에 대한 투표를 수행하여, 블록을 블록체인에 추가하는 단계; 를 포함하는 블록체인 네트워크의 장애 허용 합의 방법.

청구항 2

제1 항에 있어서, 상기 블록체인에 추가하는 단계는

상기 n개의 검증 노드들 각각에 대한 글로벌 신뢰도($\overline{C^t}$)의 합이 기지정된 글로벌 기준 비율 이상인지 판별하는 단계;

상기 글로벌 기준 비율 이상이면, 상기 블록에 대한 글로벌 신뢰도 합의가 성공한 것으로 판별하여 블록을 블록체인에 추가하는 단계;

추가된 결과를 상기 클라이언트로 전달하는 단계; 및

합의 성공 여부에 따라 검증 노드 각각에 대한 로컬 신뢰도를 재계산하는 단계; 를 포함하는 블록체인 네트워크의 장애 허용 합의 방법.

청구항 3

제2 항에 있어서, 상기 로컬 신뢰도를 재계산하는 단계는

글로벌 신뢰도 합의가 성공한 것으로 판별되면, 상기 n개의 검증 노드 중 i번째 검증 노드가 계산한 k번째 검증 노드에 대한 t번째 라운드의 로컬 신뢰도($C^t_{i,k}$)를 수학식

$$C^t_{i,k}=\begin{cases}1 & , t=1\\ \overline{C^t_k} & , V_k\in R\\ \overline{C^t_k}\left(1-\alpha\dfrac{\sum_{\forall F}\overline{C^t_l}}{\sum_{j=1}^{n}\overline{C^t_j}}\right) & , V_k\in F\end{cases}$$

(여기서 $\overline{C^t_k}$ 는 k번째 검증 노드에 대한 t번째 라운드의 글로벌 신뢰도이고, V_k는 n개의 검증 노드 중 k번째 검증 노드를 의미하고, R은 정상적인 리더 노드의 제안에 동의하는 투표를 수행한 로얄 노드의 집합을 나타내고, F는 장애 노드 집합을 나타내며, α는 패널티 가중치이다.)

에 따라 계산하는 단계; 및

글로벌 신뢰도 합의가 실패한 것으로 판별되면, 검증 노드들 각각에 대한 로컬 신뢰도를 수학식

$$C_{i,k}^{t}=\begin{cases}1 & ,\ t=1\\ C_{i,k}^{t-1} & ,\ V_k\in R\\ C_{i,k}^{t-1}\left(1-\alpha\dfrac{\sum_{\forall F}C_{i,l}^{t-1}}{\sum_{j=1}^{n}C_{i,j}^{t-1}}\right) & ,\ V_k\in F\end{cases}$$

에 따라 계산하는 단계; 를 포함하는 블록체인 네트워크의 장애 허용 합의 방법.

청구항 4

제3 항에 있어서, 상기 로컬 신뢰도를 재계산하는 단계는

상기 글로벌 신뢰도 합의 성공 여부에 따라 상기 글로벌 신뢰도에 기반하여 합의 경계(Consensus Bound)가 수학식

$$\text{Consensus success}: \quad \sum_{\forall F}\overline{C_j^t}\le\frac{\sum_{i=1}^{n}\overline{C_i^t}-1}{3}$$

$$\text{Consensus failure}: \quad \sum_{\forall F}\overline{C_j^t}>\frac{\sum_{i=1}^{n}\overline{C_i^t}-1}{3}$$

$$\text{Falsification success}: \quad \sum_{\forall F}\overline{C_j^t}\ge\frac{2\sum_{i=1}^{n}\overline{C_i^t}+1}{3}$$

에 따라 가변되는 블록체인 네트워크의 장애 허용 합의 방법.

청구항 5

제1 항에 있어서, 상기 결정 메시지를 전파하는 단계는

상기 검증 노드들 각각이 수신한 준비 메시지를 분석하여, 동일한 값을 갖는 로컬 신뢰도의 개수가 기지정된 기준 개수 이상인지 판별하는 단계;

기준 개수 이상이면, 동일한 값의 로컬 신뢰도를 현재 라운드의 글로벌 신뢰도에 반영하는 단계;

기준 개수 미만이면, 백업 로컬 신뢰도를 현재 라운드의 글로벌 신뢰도에 반영하는 단계; 및

동일한 로컬 신뢰도 값을 갖는 검증 노드들의 글로벌 신뢰도의 합이 기지정된 글로벌 기준 값 이상인지 판별하고, 글로벌 기준 값 이상이면, 결정 메시지를 다른 검증 노드로 전파하는 단계; 를 포함하는 블록체인 네트워크의 장애 허용 합의 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 블록체인 네트워크의 장애 허용 합의 방법에 관한 것으로, 블록체인 네트워크의 합의 방해요인 제거를 위한 장애 허용 합의 방법에 관한 것이다.

배 경 기 술

[0002] 블록체인 기술은 투명성, 보안성, 비가역성을 지원하는 고 신뢰도 분산화 정보저장소(DB: Database) 기술로서,

단순한 구조로 비가역성을 쉽게 확보할 수 있음에 따라, 무결성이 매우 중요시되는 금융/물류/공공분야 등에서 각광받으며 많은 프로젝트가 진행되고 있다.

[0003] 합의 알고리즘(Consensus Algorithm)은 다수 노드가 존재하는 P2P 네트워크에서 정보 불일치 발생 시 노드 간 하나의 DB를 유지하기 위해 어떤 정보를 선택할지 결정하는 기술이다. 블록체인은 합의 알고리즘을 통해 블록 생성 권한과 분기된 블록체인 선택에 대한 기법을 결정한다. 대표적 합의 알고리즘은 작업증명(Proof of Work: 이하 PoW)와 지분증명(Proof of Stake: 이하 PoS), 실용적 비잔틴 장애 허용(Practical Byzantine Fault Tolerance: 이하 PBFT) 등이 있다.

[0004] 동일한 타임 스탬프(timestamp)에서 데이터가 서로 다른 블록이 발생하는 블록체인 분기 현상이 나타나면, PoW와 PoS에서는 이후 가장 길게 연장된 블록체인을 선택한다. 그러나 이는 일시적 정보 불일치를 허용하는 방식으로 블록체인의 데이터 신뢰도를 낮추게 된다.

[0005] 반면 PBFT는 블록체인에 추가될 데이터에 대한 합의 노드 간의 정상적인 합의 수행 완료 후에만 블록을 블록체인에 추가함으로써 블록체인 데이터의 불일치를 원천 방지하여, 데이터에 대한 신뢰도를 향상시킨다. PBFT 합의 알고리즘은 약속된 행동을 하지 않는 비잔틴 장애(Byzantine Faulty) 노드가 존재할 수 있는 비동기 네트워크에서도 비잔틴 장애 노드가 일정 비율 이하에서는 정상 합의가 가능하다. 전체 검증 노드 수가 n이고, 장애 노드 수가 f인 경우, PBFT에서는 장애 노드 수(f)가 (n-1)/3 이하이면 합의에 성공할 수 있다. 즉 전체 검증 노드의 수(n)가 장애 노드 수(f)의 3배를 초과($N \geq 3f+1$)하면, 장애 노드가 포함되어도 정상적 합의가 가능하다.

[0006] 도 1은 PBFT 합의 알고리즘을 통한 합의 절차의 일예를 나타낸다.

[0007] 도 1을 참조하면, PBFT 합의 알고리즘은 요청(Request) 단계(S11), 선 준비 단계(Pre-prepare)(S12), 준비(Prepare) 단계(S13), 결정(Commit) 단계(S14) 및 응신(Reply) 단계(S15)로 구성될 수 있다.

[0008] 블록체인 네트워크에서 다수의 노드 중 클라이언트(Client)(120)에서 전송된 트랜잭션 요청을 검증하고 합의하여 블록에 추가하는 역할은 검증 노드들(Validating Nodes)(110)이 담당한다. 도1 에서는 일예로 블록체인 네트워크에 4개의 검증 노드(111 ~ 114)가 존재하고, 4개의 검증 노드(111 ~ 114) 중 제1 검증 노드(111)가 클라이언트(120)로부터 트랜잭션 요청을 인가받는 리더 노드이며, 나머지 제2 내지 제4 검증 노드(112 ~ 114)는 리더 노드(111)와 함께 요청된 랜잭션에 대해 합의 검증하는 백업 노드이다.

[0009] PBFT 합의 알고리즘의 요청 단계(S11)에서 리더 노드(111)는 적어도 하나의 클라이언트(120)로부터 데이터의 상태 변환, 즉 트랜잭션을 요청하는 데이터를 인가받아 종합하고, 검증 및 정렬한다. 그리고 선 준비 단계(S12)에서 리더 노드(111)는 인가된 블록을 나머지 검증 노드들(112 ~ 114), 즉 백업 노드들로 전파한다. 준비 단계(S13)에서 백업 노드들(112 ~ 114) 각각은 리더 노드(111)에서 블록을 검증하고, 검증 결과가 참이면, 각각 다른 검증 노드들(111 ~ 114)로 준비 메시지를 전파한다. 결정 단계(S14)에서 각 검증 노드들(111 ~ 114)은 2f개 이상의 노드로부터 같은 값을 받으면 결정 메시지를 다른 노드들에게 전파한다. 응신 단계(S15) 단계에서 검증 노드들(111 ~ 114) 각각은 2f+1개 이상의 다른 노드들로부터 같은 값의 결정 메시지를 받으면 해당 블록을 체인에 추가하고, 결과를 클라이언트(120)에게 전달한다. 이에 클라이언트는 f+1 이상의 다른 노드들로부터 동일한 결과를 받으면 해당 결과가 처리된 것으로 확인한다.

[0010] 이와 같이 PBFT에서는 전체 검증 노드(n)의 2/3를 초과하는 노드를 확보해야만 블록 데이터의 변경이 가능하므로, 51% 이상의 노드를 확보하면 데이터 변조가 가능한 PoW 및 PoS 보다 데이터 변조 공격에 강하지만, 데이터 변조 공격이 전체 검증 노드의 1/3 이상 노드만 확보해도 정상 합의를 실패하게 만들고 정상 합의로 복귀하지 못하도록 교착 상태로 만들 수 있는 문제점이 있다.

선행기술문헌

특허문헌

[0011] (특허문헌 0001) 한국 공개 특허 제10-2018-0113140호 (2018.10.15 공개)

발명의 내용

해결하려는 과제

[0012] 본 발명의 목적은 PBFT 합의 알고리즘을 기반으로 신뢰 평가 모델을 접목하여, 비정상 행위에 대한 벌칙 부과를 통해 합의 성공률 향상 및 합의 교착상태에서 정상 합의로 회귀할 수 있도록 하는 블록체인 네트워크의 장애 허용 합의 방법을 제공하는데 있다.

과제의 해결 수단

[0013] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 블록체인 네트워크를 위한 장애 허용 합의 방법은 n개의 검증 노드 중 기지정된 리더 노드가 적어도 하나의 클라이언트로부터 전송된 트랜잭션 요청이 포함된 블록이 수신되면, 상기 리더 노드에 대해 이전 투표 결과로부터 획득된 로컬 신뢰도인 리더 신뢰도를 상기 블록에 포함하여 나머지 검증 노드인 백업 노드들로 전파하는 단계; 상기 백업 노드들 각각이 이전 투표 결과로부터 획득된 자신에 대한 로컬 신뢰도인 백업 신뢰도와 상기 리더 신뢰도를 비교하여, 서로 상이하면 다른 검증 노드들로 리더 신뢰도를 상기 백업 신뢰도로 변경한 준비 메시지를 전파하는 단계; 상기 검증 노드들 각각이 수신한 준비 메시지를 분석하여, 동일한 값을 갖는 로컬 신뢰도의 개수가 기지정된 기준 개수 이상이면, 다른 검증 노드들로 상기 로컬 신뢰도를 글로벌 신뢰도에 적용하여 결정 메시지를 전파하는 단계; 및 상기 검증 노드들 각각이 결정 메시지에 포함된 글로벌 신뢰도의 합을 기반으로 트랜잭션 요청에 대한 투표를 수행하여, 블록을 블록체인에 추가하는 단계; 를 포함한다.

[0014] 상기 블록체인에 추가하는 단계는 상기 n개의 검증 노드들 각각에 대한 글로벌 신뢰도($\overline{C^t}$)의 합이 기지정된 글로벌 기준 비율 이상인지 판별하는 단계; 상기 글로벌 기준 비율 이상이면, 상기 블록에 대한 글로벌 신뢰도 합의가 성공한 것으로 판별하여 블록을 블록체인에 추가하는 단계; 추가된 결과를 상기 클라이언트로 전달하는 단계; 및 합의 성공 여부에 따라 검증 노드 각각에 대한 로컬 신뢰도를 재계산하는 단계; 를 포함할 수 있다.

[0015] 상기 로컬 신뢰도를 재계산하는 단계는 글로벌 신뢰도 합의가 성공한 것으로 판별되면, 상기 n개의 검증 노드 중 i번째 검증 노드가 계산한 k번째 검증 노드에 대한 t번째 라운드의 로컬 신뢰도($C^t_{i,k}$)를 수학식

[0016]
$$C_{i,k}^{t}=\begin{cases}1 & ,t=1\\ \overline{C_k^t} & ,V_k\in R\\ \overline{C_k^t}\left(1-\alpha\dfrac{\sum_{\forall F}\overline{C_l^t}}{\sum_{j=1}^{n}\overline{C_j^t}}\right) & ,V_k\in F\end{cases}$$

[0017] (여기서 $\overline{C_k^t}$ 는 k번째 검증 노드에 대한 t번째 라운드의 글로벌 신뢰도이고, V_k는 n개의 검증 노드 중 k번째 검증 노드를 의미하고, R은 정상적인 리더 노드의 제안에 동의하는 투표를 수행한 로얄 노드의 집합을 나타내고, F는 장애 노드 집합을 나타내며, α는 패널티 가중치이다.)에 따라 계산하는 단계; 및 글로벌 신뢰도 합의가 실패한 것으로 판별되면, 상기 검증 노드들 각각에 대한 로컬 신뢰도를 수학식

[0018]
$$C_{i,k}^{t}=\begin{cases}1 & ,t=1\\ C_{i,k}^{t-1} & ,V_k\in R\\ C_{i,k}^{t-1}\left(1-\alpha\dfrac{\sum_{\forall F}C_{i,l}^{t-1}}{\sum_{j=1}^{n}C_{i,j}^{t-1}}\right) & ,V_k\in F\end{cases}$$

[0019] 에 따라 계산하는 단계; 를 포함할 수 있다.

[0020] 상기 로컬 신뢰도를 재계산하는 단계는 상기 글로벌 신뢰도 합의 성공 여부에 따라 상기 글로벌 신뢰도에 기반하여 합의 경계(Consensus Bound)가 수학식

Consensus success : $$\sum_{\forall F}\overline{C_j^t} \leq \frac{\sum_{i=1}^{n}\overline{C_i^t}-1}{3}$$

Consensus failure : $$\sum_{\forall F}\overline{C_j^t} > \frac{\sum_{i=1}^{n}\overline{C_i^t}-1}{3}$$

Falsification success : $$\sum_{\forall F}\overline{C_j^t} \geq \frac{2\sum_{i=1}^{n}\overline{C_i^t}+1}{3}$$

[0021]

[0022] 에 따라 가변될 수 있다.

[0023] 상기 결정 메시지를 전파하는 단계는 상기 검증 노드들 각각이 수신한 준비 메시지를 분석하여, 동일한 값을 갖는 로컬 신뢰도의 개수가 기지정된 기준 개수 이상인지 판별하는 단계; 상기 기준 개수 이상이면, 동일한 값의 로컬 신뢰도를 현재 라운드의 글로벌 신뢰도에 반영하는 단계; 상기 기준 개수 미만이면, 백업 로컬 신뢰도를 현재 라운드의 글로벌 신뢰도에 반영하는 단계; 및 동일한 로컬 신뢰도 값을 갖는 검증 노드들의 글로벌 신뢰도의 합이 기지정된 글로벌 기준 값 이상인지 판별하고, 글로벌 기준 값 이상이면, 결정 메시지를 다른 검증 노드로 전파하는 단계; 를 포함할 수 있다.

발명의 효과

[0024] 따라서, 본 발명의 실시예에 따른 블록체인 네트워크의 합의 방해요인 제거를 위한 장애 허용 합의 방법은 블록체인의 합의 노드 중 비잔틴 장애 노드들의 합의에 대한 영향력을 낮춰 교착 상태에서 정상 합의로 회귀할 수 있도록 함으로써, 정상적인 합의의 성공률을 높일 수 있다.

도면의 간단한 설명

[0025] 도 1은 PBFT 합의 알고리즘을 통한 합의 절차의 일예를 나타낸다.

도 2는 본 발명의 일 실시예에 따른 블록체인 네트워크 구성을 나타낸다.

도 3은 블록체인 네트워크의 합의 방해요인 제거를 위한 장애 허용 합의 방법을 나타낸다.

도 4는 본 발명의 일 실시예에 따른 수정된 블록 구조를 나타낸다.

도5 는 본 발명의 일 실시예에 따른 장애 허용 블록체인 단말의 개략적 구조를 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0026] 본 발명과 본 발명의 동작상의 이점 및 본 발명의 실시에 의하여 달성되는 목적을 충분히 이해하기 위해서는 본 발명의 바람직한 실시예를 예시하는 첨부 도면 및 첨부 도면에 기재된 내용을 참조하여야만 한다.

[0027] 이하, 첨부한 도면을 참조하여 본 발명의 바람직한 실시예를 설명함으로써, 본 발명을 상세히 설명한다. 그러나, 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 설명하는 실시예에 한정되는 것이 아니다. 그리고, 본 발명을 명확하게 설명하기 위하여 설명과 관계없는 부분은 생략되며, 도면의 동일한 참조부호는 동일한 부재임을 나타낸다.

[0028] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라, 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "...부", "...기", "모듈", "블록" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[0029] 도 2는 본 발명의 일 실시예에 따른 블록체인 네트워크 구성을 나타낸다.

[0030] 도 2를 참조하면, 본 실시예에 따른 블록체인 네트워크(200)는 다수의 노드 중 메쉬 타입(mesh-type)으로 상호 통신이 가능한 n(여기서 n은 자연수)개의 검증 노드(211 ~ 21n)를 포함하여 다수의 클라이언트들로부터 전송되

는 트랜잭션 요청을 검증하고 합의하여 블록에 추가할 수 있다. 도 2에서는 설명의 편의를 위하여 검증 노드(211 ~ 21n)를 4개만 도시하였으나, 검증 노드의 개수는 다양하게 조절될 수 있다. 그리고 다수의 검증 노드(211 ~ 21n) 중 제1 검증 노드(211)는 다수의 클라이언트(221 ~ 22m) 중 적어도 하나의 클라이언트로부터 트랜잭션 요청을 인가받는 리더 노드이며, 나머지 제2 내지 제4 검증 노드(212 ~ 21n)는 백업 노드인 것으로 가정한다.

[0031] 상기한 바와 같이 다수의 검증 노드(211 ~ 21n) 중 리더 노드(211)는 적어도 하나의 클라이언트(221 ~ 22m)로부터 인가된 트랜잭션 요청을 검증 및 정렬하여 다른 검증 노드들인 백업 노드들(212 ~ 21n)로 전파하고, 다수의 검증 노드(211 ~ 21n)간의 합의를 통하여 블록을 확정하고, 블록체인에 추가하는 절차로 블록을 연장 및 유지한다.

[0032] 블록체인에 참여하고 있는 모든 n개 검증 노드(211 ~ 21n)는 합의 라운드마다 합의에 참여하며, 특정시점(t_0)부터 활동하는 악성 노드는 블록 변조 시도 또는 합의 미참여를 수행한다. 악성 노드가 정상적으로 합의에 참여하는 것은 합의에 영향이 없으며, 악의적 의도를 관철하려면 더 많은 검증 노드들에게 메시지를 보내야 효과적이므로 합의 단계별로 다른 검증 노드에게 정상 메시지와 변조 메시지를 동시에 보내는 것은 고려하지 않는다. 이때 정상 노드가 네트워크 환경에 따라 시간 지연(time delay), 네트워크 혼잡(network congestion) 등에 의해 합의에 참여 실패하게 되더라도, 합의에 부정적 영향을 미치므로 패널티(penalty)를 부여한다.

[0033] 블록체인 네트워크의 n개의 검증 노드(211 ~ 21n) 중 사전에 결정된 리더 노드(211)가 블록을 생성하며, n개 검증 노드(211 ~ 21n) 중 장애(Faulty) 노드의 개수가 f개일 때, 검증 노드 집합(V)과 장애 노드 집합(F), 정상적인 리더 노드(211)의 제안에 동의하는 투표를 한 로얄(Royal) 노드의 집합(R)은 각각 $V=\{V_k|k=1, \ldots, n\}$, $F=\{F_k|k=1, \ldots, f\}$, $R=\{R_k|k=1, \ldots, n-f\}$로 정의될 수 있다.

[0034] 블록체인 네트워크의 n개의 검증 노드(211 ~ 21n) 각각은 결정(commit) 단계에서 수집한 투표 정보를 바탕으로 신뢰도 평가를 실시하여 로컬 신뢰도(Local Credibility)($C^t_{i,k}$)를 계산한다. 여기서 i번째 검증 노드(21i)가 계산한 전체 검증 노드에 대한 로컬 신뢰도 집합(C^t_i)은 수학식 1과 같이 표현된다.

수학식 1

[0035] $$C_i^t = \left\{ C_{i,k}^t | k = 1, \cdots, n \right\},\ 1 \le i \le n \ \text{ and } \ 2 \le t$$

[0036] 각 검증 노드들(211 ~ 21n)은 t-1 라운드에서 투표를 통해 평가한 로컬 신뢰도($C^t_{i,k}$)를 t 라운드까지 유지한다. 리더 노드(211)는 t 라운드 시 자신의 로컬 신뢰도(C^t_1)를 블록과 함께 제안한다. 검증 노드(211 ~ 21n) 간 합의로 결정된 신뢰도는 글로벌 신뢰도로 인정되며 수학식 2로 표현도리 수 있다.

수학식 2

[0037] $$\overline{C^t} = \left\{ \overline{C_k^t} | k = 1, \cdots, n \right\},\ 2 \le t$$

[0038] 블록체인의 최초의 블록인 제네시스 블록(Genesis block)에서 이전 노드에 대한 신뢰도는 1이며, 두번째 블록부터 이전 라운드의 투표결과에 따라 신뢰도를 계산한다. 먼저 정상적인 리더 노드(211)의 제안에 동의하는 투표를 했을 경우 해당 노드는 로얄 노드(R)로 판단하며 이전 라운드의 신뢰도를 유지한다.

[0039] 그러나 잘못된 투표를 하거나 투표를 하지 않은 장애 노드(F)로 판단되면, 이전 라운드의 전체 장애 노드의 신뢰도를 전체 검증 노드의 신뢰도로 나눈 값에 패털티 가중치(α)를 곱한 값만큼 감소시킨다. 이때 신뢰도 합의 절차(Credibility Consensus Procedures)를 통해 정상적으로 글로벌 신뢰도가 결정된 경우, k번째 노드의 t-1 라운드 로컬 신뢰도($C^{t-1}_{i,k}$)는 글로벌 신뢰도의 k번째 검증 노드의 t 라운드 글로벌 신뢰도($\overline{C_k^t}$)와 같다. 이를

통해 로컬 신뢰도($C^{t}_{i,k}$)는 수학식 3과 같이 계산된다.

수학식 3

$$C^{t}_{i,k}=\begin{cases}1 & , t=1\\ \overline{C^{t}_{k}} & , V_k \in R\\ \overline{C^{t}_{k}}\left(1-\alpha\dfrac{\sum_{\forall F}\overline{C^{t}_{l}}}{\sum_{j=1}^{n}\overline{C^{t}_{j}}}\right) & , V_k \in F\end{cases}$$

[0040]

[0041] 반면, 글로벌 신뢰도의 합의가 실패한다면, 이전 라운드의 로컬 신뢰도를 활용하여 수학식 4와 같이 해당 라운드의 신뢰도를 재계산한다.

수학식 4

$$C^{t}_{i,k}=\begin{cases}1 & , t=1\\ C^{t-1}_{i,k} & , V_k \in R\\ C^{t-1}_{i,k}\left(1-\alpha\dfrac{\sum_{\forall F}C^{t-1}_{i,l}}{\sum_{j=1}^{n}C^{t-1}_{i,j}}\right) & , V_k \in F\end{cases}$$

[0042]

[0043] 수학식 3 및 4에서 장애 노드의 개수(f)가 증가할수록 정상 합의에 실패할 확률이 증가한다. 그러므로 장애 노드의 신뢰도 합의 증가에 비례하여 장애 노드들과 전체 검증 노드들(211 ~ 21n)의 신뢰도 합의 비율만큼 패널티를 증가시킴으로써, 장애 노드 합의 영향력을 감소시켜 합의 성공률을 높일 수 있다.

[0044] 이는 다수의 검증 노드에 의한 합의 경계를 적응적으로 변화시켜, 합의 방해 요인인 장애 노드의 존재에도 불구하고, 성공률 향상 및 합의 교착상태에서 정상 합의로 회귀할 수 있도록 하며, 본 실시예에 따른 장해 허용 합의 알고리즘을 적응적 합의 경계(Adaptive Consensus Bound) PBTF(이하: ACB-PBFT) 알고리즘이라 한다.

[0045] 각 검증 노드의 신뢰 값(Trust value)을 의미하는 신뢰도는 각 노드별로 계산된다. 계산된 신뢰도를 이용하여 전체 검증 노드가 하나의 신뢰 값을 공유하기 위해서는 3 단계 프로토콜(3-phase protocol) 방식으로 합의를 수행한다.

[0046] 도 3은 블록체인 네트워크의 합의 방해요인 제거를 위한 장애 허용 합의 방법을 나타내고, 도 4는 본 발명의 일 실시예에 따른 수정된 블록 구조를 나타낸다.

[0047] 도 3의 장애 허용 합의 방법을 설명하기에 앞서, 도 4를 참조하여 본 실시예에 따라 수정된 블록 구조를 우선 설명하면, 블록은 블록 헤더(Block Header)(410)와 블록 바디(Block Body)(420)로 구분된다. 그리고 블록 헤더(410)는 버전 필드(Version)(411), 이전 블록 해시 필드(Hash of Prev. Block)(404), 머클 루트 해시 필드(Hash of Merkle Root)(405) 및 타임 스탬프(Time Stamp)(406)로 구성될 수 있다. 한편, 블록 바디(420)는 트랜잭션 카운터(Trasaction Counter)(421), 신뢰도 트랜잭션(Credibility Transaction)(422) 및 트랜잭션(Transactions)(423)으로 구성될 수 있다.

[0048] 도 4에 도시된 본 실시예에 따른 블록 구조를 기존의 대표적인 블록체인 시스템인 비트코인의 블록 구조와 비교하면, 본 실시예의 블록체인 네트워크는 블록 생성자인 리더 노드를 비경쟁형으로 선정하므로, 블록 생성자를 결정하기 위해 비트코인에서 사용되는 난이도(Difficulty) 필드와 논스(Nonce) 필드가 제거되었다. 또한 본 실시예에 따른 ACB-PBFT는 각 검증 노드의 투표권(Voting Power)을 의미하는 신뢰도(Credibility)를 사용하므로, 이하에서 설명하는 신뢰도 합의 절차(Credibility Consensus Procedures)를 통해 합의된 각 검증 노드의 신뢰도

전체 집합인 글로벌 신뢰도를 블록 바디(420) 내 신뢰도 트랜잭션 필드 (422)에 기록하여 블록체인을 유지하고 있는 전체 검증 노드가 동일한 글로벌 신뢰도를 공유할 수 있도록 한다.

[0049] 이하에서는 도 2 및 도 4를 참조하여, 도 3의 장애 허용 합의 방법을 설명한다. 본 실시예에 따른 장애 허용 합의 방법 또한 기본적으로 도 1에 도시된 PBFT 알고리즘과 마찬가지로, 요청 단계, 선 준비 단계, 준비 단계, 결정 단계 및 응신 단계를 포함하여 수행될 수 있다.

[0050] 우선 신뢰도 합의 절차를 수행한다. 요청 단계(미도시)에서 적어도 하나의 클라이언트로부터 리더 노드(211)로 트랜잭션 요청이 전송되면, 선 준비 단계에서 리더 노드(211)는 이전 라운드(t-1)의 투표 결과로 계산된 리더 로컬 신뢰도(C_L^{t-1})를 도 4의 블록 데이터의 신뢰도 트랜잭션 필드(422)에 기록하여, 블록을 나머지 검증 노드들인 백업 노드들(212 ~ 21n)에게 전파하여 제안한다(S31).

[0051] 그리고 준비 단계에서 블록을 수신한 백업 노드들(212 ~ 21n) 각각은 이전 라운드(t-1)에서 계산된 자신의 백업 로컬 신뢰도(C_i^{t-1})와 리더 노드(211)에서 전송된 블록의 신뢰도 트랜잭션 필드(422)에 기록된 리더 로컬 신뢰도(C_L^{t-1})가 동일한지 판별한다(S32).

[0052] 판별 결과, 자신의 백업 로컬 신뢰도(C_i^{t-1})와 리더 로컬 신뢰도(C_L^{t-1})가 동일하면, 리더 로컬 신뢰도(C_L^{t-1})를 선택하고, 선택된 리더 로컬 신뢰도(C_L^{t-1})가 기록된 블록을 준비 메시지로서 리더 노드(211)를 제외한 다른 백업 노드들로 전파한다(S33). 그러나 백업 로컬 신뢰도(C_i^{t-1})와 리더 로컬 신뢰도(C_L^{t-1})가 서로 상이하면, 블록의 신뢰도 트랜잭션 필드(422)에 백업 로컬 신뢰도(C_i^{t-1})를 기록하여 리더 노드(211)를 제외한 다른 검증 노드들로 전파한다(S34).

[0053] 결정 단계에서 모든 검증 노드(211 ~ 21n)는 자신이 선택한 로컬 신뢰도와 다른 검증 노드들로부터 전파된 준비 메시지의 로컬 신뢰도(C_i^{t-1})를 분석한다(S35). 그리고 분석된 로컬 신뢰도에서 동일한 값을 갖는 로컬 신뢰도의 개수가 전체 검증 노드(211 ~ 21n)의 개수(n)에 대해 기지정된 기준 개수 이상인지 판별한다(S36). 여기서 기준 개수는 일예로 2(n-1)/3로 설정될 수 있다.

[0054] 만일 동일한 값을 갖는 로컬 신뢰도(C_k)의 개수가 기준 개수 이상이면, 해당 검증 노드는 동일한 값의 로컬 신뢰도를 현재 라운드의 글로벌 신뢰도($\overline{C^t}$)에 반영하여, 즉 로컬 신뢰도를 블록의 신뢰도 트랜잭션 필드(422)에 기록하여 결정 메시지로서 다른 노드로 전파한다(S37). 그러나 동일한 값을 갖는 로컬 신뢰도의 개수가 기준 개수 미만이면, 백업 로컬 신뢰도(C_i^{t-1})를 현재 라운드의 글로벌 신뢰도($\overline{C^t}$)에 반영하여 결정 메시지를 다른 검증 노드로 전파한다(S38).

[0055] 이때 검증 노드(211 ~ 21n) 각각은 준비 메시지를 전송한 검증 노드들, 즉 동일한 로컬 신뢰도 값을 갖는 검증 노드들의 글로벌 신뢰도의 합이 기지정된 글로벌 기준 값(예를 들면, $2(\sum_{k=1}^{n}\overline{C_k^t}-1)/3$) 이상인지 판별하고, 글로벌 기준 값 이상이면, 결정 메시지를 다른 검증 노드로 전파하도록 구성될 수 있다.

[0056] 이러한 과정을 통해 리더 노드(211)가 제안한 리더 신뢰도 또는 전체 검증 노드 중 2f+1개 이상의 검증 노드가 공유하는 동일한 로컬 신뢰도는 글로벌 신뢰도 인정받고, 인정된 글로벌 신뢰도 값이 블록의 신뢰도 트랜잭션 필드(422)에 기록되어 된다.

[0057] 본 실시예에서 글로벌 신뢰도($\overline{C^t}=\{\overline{C_k^t}|k=1,\cdots,n\}$)는 각 검증 노드(211 ~ 21n)의 투표 가중치로 이용될 수 있다. 다수의 검증 노드(211 ~ 21n) 각각은 자신을 포함한 다수의 검증 노드 중 동일한 결과 메시지를 전파한 검증 노드들의 글로벌 신뢰도의 합($\sum_{k=1}^{n}\overline{C_k^t}$)이 기지정된 글로벌 기준 비율 이상인지 판별하고, 다수의 검증 노드(211 ~ 21n) 각각은 글로벌 신뢰도의 합($\sum_{k=1}^{n}\overline{C_k^t}$)이 글로벌 기준 비율 이상이면, 합의가 성공된 것으로 판별하여 블록을 블록체인에 추가하고, 추가된 결과를 클라이언트로 전달한다(S40). 여기서 기준 비율은 일예로

$2(\sum_{k=1}^{n}\overline{C_k^t}-1)/3+1$ 로 설정될 수 있다.

[0058] 상기한 바와 같이, 본 실시예에 따른 ACB-PBFT 합의 방법은 다수의 검증 노드(211 ~ 21n)에 대한 합의 성공을 판단하는 합의 경계(Consensus Bound)가 적응적으로 변화하게 되며, 각각의 합의 경계는 수학식 5와 같이 표현될 수 있다.

수학식 5

[0059]

$$\text{Consensus success}: \quad \sum_{\forall F}\overline{C_j^t} \le \frac{\sum_{i=1}^{n}\overline{C_i^t}-1}{3}$$

$$\text{Consensus failure}: \quad \sum_{\forall F}\overline{C_j^t} > \frac{\sum_{i=1}^{n}\overline{C_i^t}-1}{3}$$

$$\text{Falsification success}: \quad \sum_{\forall F}\overline{C_j^t} \ge \frac{2\sum_{i=1}^{n}\overline{C_i^t}+1}{3}$$

[0060] 그리고 블록에 대한 투표 결과에 따라 모든 검증 노드(211 ~ 21n)에 대한 로컬 신뢰도(C^t_i)를 수학식 3 또는 4에 따라 재계산한다(S41).

[0061] 도5 는 본 발명의 일 실시예에 따른 장애 허용 블록체인 단말의 개략적 구조를 나타낸다.

[0062] 도5 를 참조하면, 단말은 정보교환 및 합의수행을 위해 정보 입력부(501), 메모리(502), CPU(503), 메시지 처리부(504), 정보 출력부(505)를 포함할 수 있다.

[0063] 정보 입력부(501)는 다른 노드로부터 전달받은 투표 정보를 수신하는 역할을 수행한다.

[0064] 메모리(502)는 CPU에서 처리한 정보들을 저장한다. 구체적으로 메모리는 각 노드의 투표 정보, 계산된 신뢰도 정보, 블록체인 데이터 등의 정보를 저장한다.

[0065] CPU(503)는 수신된 투표 정보를 메시지 처리부(504)로 송신하며, 메시지 처리부에서 수신한 투표 정보를 정보 출력부(505)로 송신한다. 또한 정보 입력부(501), 정보 출력부(505), 메모리(502), 메시지 처리부(504)에 대한 동작을 제어한다.

[0066] 메시지 처리부(504)는 타 노드의 투표 정보를 분석하여 신뢰도 정보를 계산 및 합의 단계별 수신되는 메시지를 비교 검증하는 역할을 수행한다.

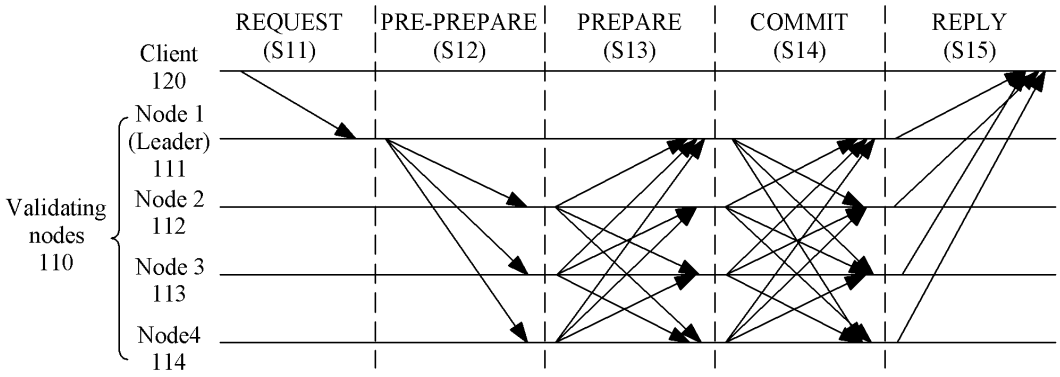
[0067] 본 발명에 따른 방법은 컴퓨터에서 실행 시키기 위한 매체에 저장된 컴퓨터 프로그램으로 구현될 수 있다. 여기서 컴퓨터 판독가능 매체는 컴퓨터에 의해 액세스 될 수 있는 임의의 가용 매체일 수 있고, 또한 컴퓨터 저장 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함하며, ROM(판독 전용 메모리), RAM(랜덤 액세스 메모리), CD(컴팩트 디스크)-ROM, DVD(디지털 비디오 디스크)-ROM, 자기 테이프, 플로피 디스크, 광데이터 저장장치 등을 포함할 수 있다.

[0068] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다.

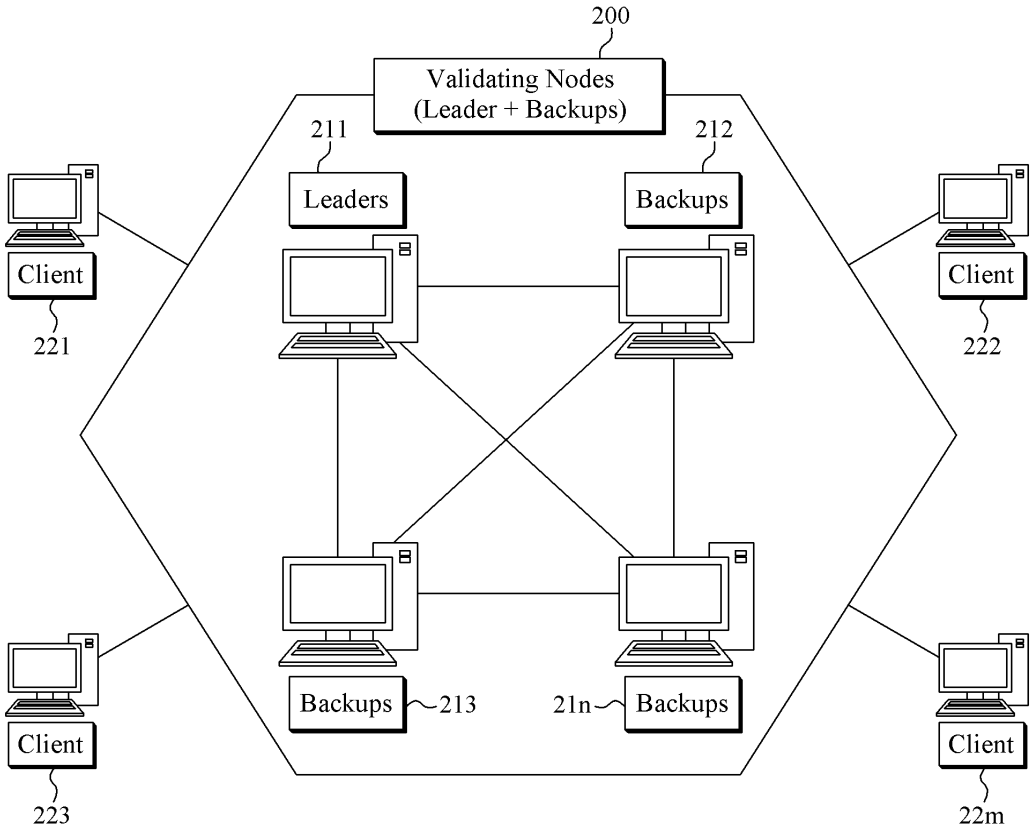
[0069] 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 청구범위의 기술적 사상에 의해 정해져야 할 것이다.

도면

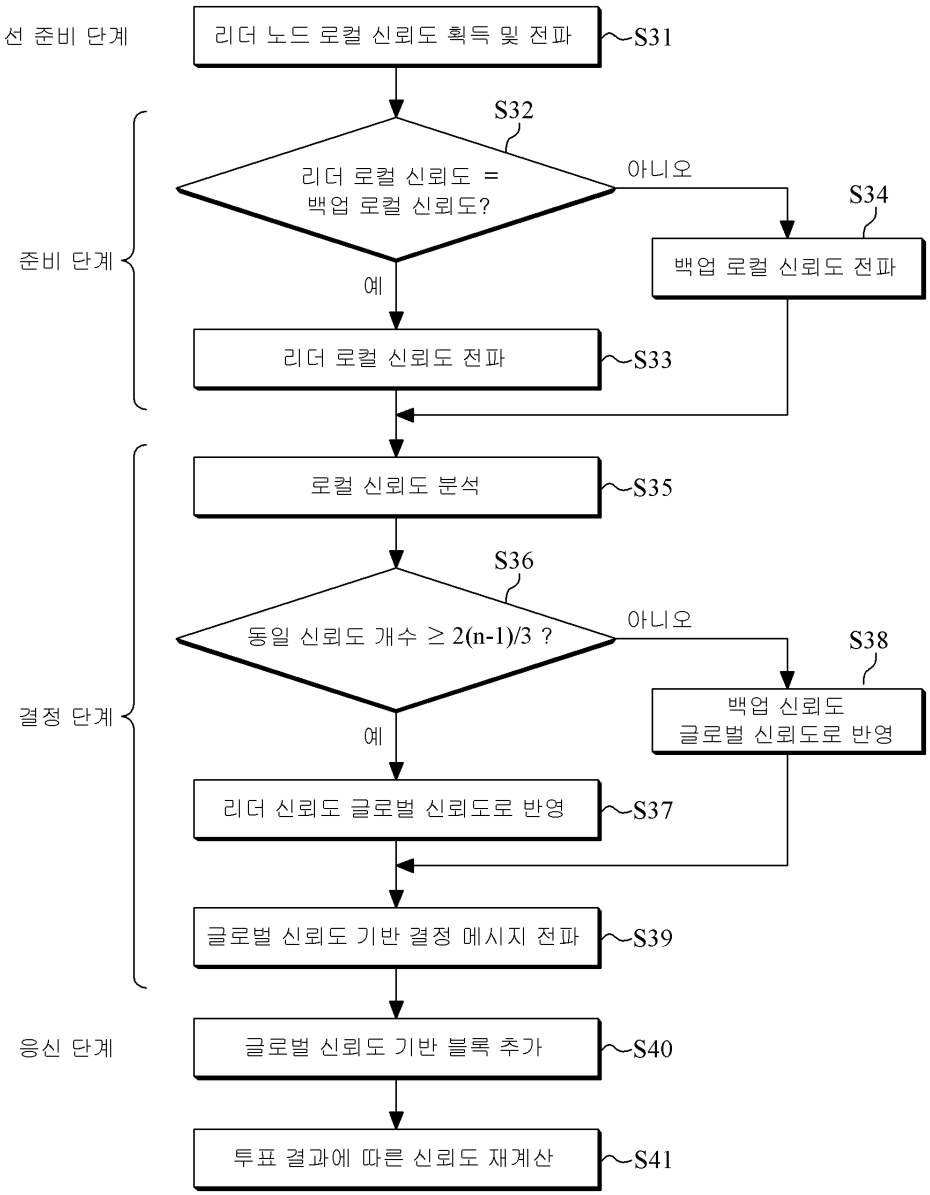
도면1


REQUEST
(S11)
PRE-PREPARE
(S12)
PREPARE
(S13)
COMMIT
(S14)
REPLY
(S15)
Client
120
Validating
nodes
110
Node 1
(Leader)
111
Node 2
112
Node 3
113
Node4
114

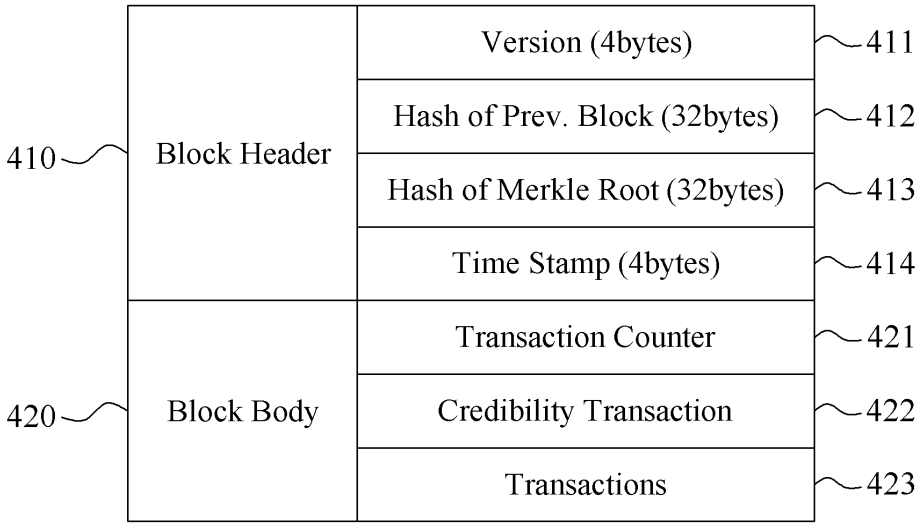
도면2


200
Validating Nodes
(Leader + Backups)
211
212
Leaders
Backups
Client
221
Client
222
Backups
213
21n
Backups
Client
223
Client
22m

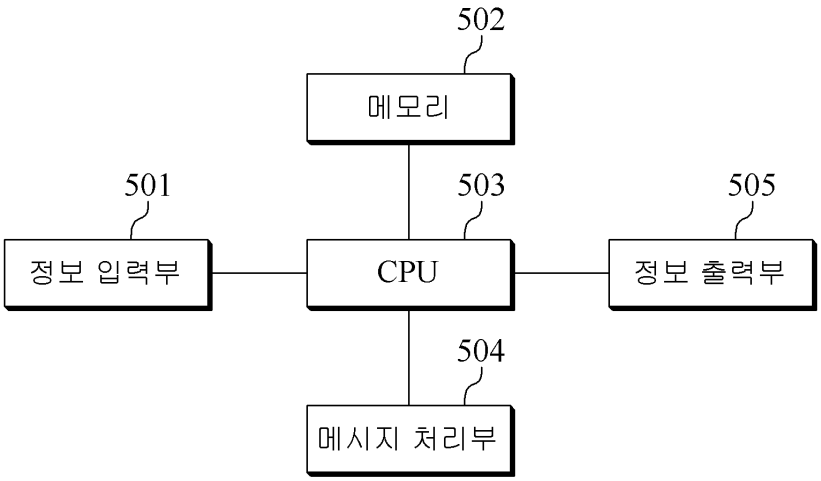
도면3


선 준비 단계
리더 노드 로컬 신뢰도 획득 및 전파
S31
S32
리더 로컬 신뢰도 =
백업 로컬 신뢰도?
아니오
S34
백업 로컬 신뢰도 전파
준비 단계
예
리더 로컬 신뢰도 전파
S33
로컬 신뢰도 분석
S35
S36
동일 신뢰도 개수 ≥ 2(n-1)/3 ?
아니오
S38
백업 신뢰도
글로벌 신뢰도로 반영
결정 단계
예
리더 신뢰도 글로벌 신뢰도로 반영
S37
글로벌 신뢰도 기반 결정 메시지 전파
S39
응신 단계
글로벌 신뢰도 기반 블록 추가
S40
투표 결과에 따른 신뢰도 재계산
S41

도면4


410
Block Header
Version (4bytes)
411
Hash of Prev. Block (32bytes)
412
Hash of Merkle Root (32bytes)
413
Time Stamp (4bytes)
414
420
Block Body
Transaction Counter
421
Credibility Transaction
422
Transactions
423

도면5


502
메모리
501
503
505
정보 입력부
CPU
정보 출력부
504
메시지 처리부